Corporate Policy

Policy: **I.T. Security Policy**

Main Contact: **Clerk**

Last Revision: **New**

Policy Statement

The Corporation of the Township of Whitewater Region provides access to information technology for legitimate business use in the course of assigned duties. The Township requires that employees conduct themselves responsibly and professionally in their use of information technology, and respect the software licensing agreements, copyrights, privacy, rights and privileges of others.

Purpose

This policy is intended to ensure the confidentiality, integrity and availability of data and resources through the use of effective and established IT security processes and procedures based on best practices.

Definitions

In this policy, the following terms have the meanings set out below:

“Information technology” is the use of computers to store, retrieve, transmit, and manipulate data.

“I.T. Services” includes the Chief Administrative Officer, the Clerk or the Treasurer of the Township of Whitewater Region, and I.T. contracted services.

“Information Users” include all employees of the Township who access or receive information produced, stored, or communicated by the Township’s information technology systems. Users also include all individuals, who by nature of their relationship with the Township (e.g., contractors, vendors, service providers, consultants, etc.) are entrusted with sensitive or confidential information

“Township” means the Corporation of the Township of Whitewater Region

Policy Requirements

1.0 Use of Information

1.1 All information stored or recorded on or through use of the Township information technology, including information marked private, personal and/or confidential, belongs to the Township and may be accessed for regular business, security, or audit purposes without prior notice to the user. Information in an electronic format must be treated in the same manner as paper records. Township retention schedules apply to electronic information, email and electronic information should not be destroyed, except in accordance with those schedules. Information may be required to be released to the public if it is requested under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

1.2 Any software to be installed within the Township must first be approved by I.T. Services.

1.3 To prevent unauthorized access to the Township’s information technology assets, user accounts and passwords have been assigned to users for the Township systems to which they require access to perform their duties. Each user is responsible for the security of their assigned passwords.

1.4 Passwords must be a minimum of 8 characters in length and must include a small letter, a capital letter, a special character and a number. Users are required to change their network and application passwords every 90 days.

1.5 All desktops and laptops at the Township must have anti-virus software running on them at all times while in operation. Users should contact I.T. Services immediately if they receive a virus warning or require assistance with virus scanning.

1.6 Users should not express personal opinions in public forums on the Internet while using a Township email address. Users must not knowingly access web sites that might bring the Township into disrepute, such as those which contain material which violates any Township policies or contain pornography, gaming, discriminatory material (e.g. racist, sexist, hate literature etc.) or any material which contravenes the Ontario Human Rights Act, Criminal Code or any other Federal or Provincial law. Employees are prohibited from using the Township’s Internet connection and/or their Township email account to run their own business/company.

1.7 Information users should exercise caution when opening email attachments particularly if the source is unknown. Information users must not possess, send or forward inappropriate email, graphics or sound files. Unwanted advertising (i.e. SPAM) should be deleted.

1.8 I.T. Services may access a user's email at any time without notice to the user.

1.9 Laptop computers and handheld devices that are used for Township business must be secured and protected with a power-on password to prevent unauthorized access. Laptops must have a password lockout after 15 minutes of non-usage.

1.10 Non-staff are prohibited from connecting to the Township's network. If staff have a requirement for a public member to use the Township's network facilities, they must contact I.T. Services to make arrangements. Consultants must not be given passwords to the network.

Monitoring

The Clerk, as staff person leading I.T. Services, will monitor this policy.

Authority

Section 224 of the *Municipal Act, 2001* states the role of Council includes the development and evaluation of policies and programs of the municipality.

Contact

Clerk
P.O. Box 40, 44 Main Street
Cobden ON K0J 1K0
(613) 646-2282

Change History

Policy Name	Effective Date	Significant Changes	By-law No.
I.T. Security Policy	October 2, 2019	New Policy	19-10-1214